Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Dr. Christopher Wolf
Alexander Meurer, Florian Giesen

RUHR UNIVERSITÄT BOCHUM RUB

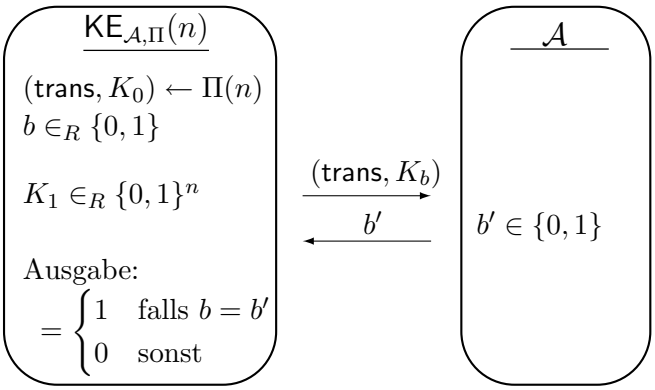
Hausübungen zur Vorlesung

Kryptographie 2

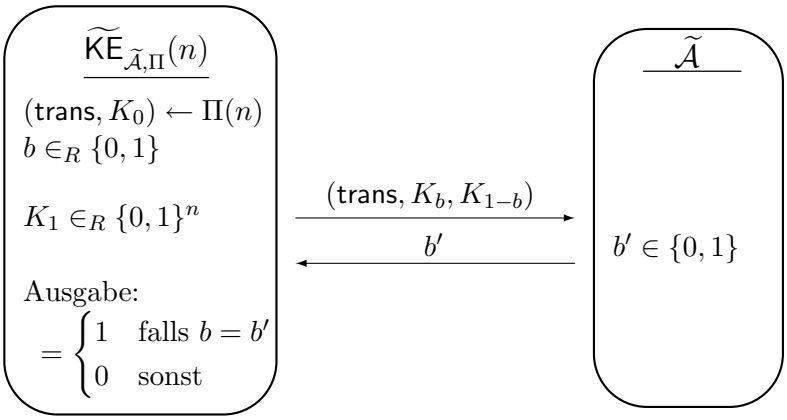
SS 2010

Blatt 2 / 28. April 2010 / Abgabe 10. Mai, 13:00 Uhr, Kasten NA 02

AUFGABE 1. Definitionssache. (5 Punkte)
Wir erinnern uns kurz an das Spiel für ein Schlüsselaustausch-Protokoll Π:



Wir ändern diese Definition nun wie folgt ab: Der Angreifer $\widetilde{\mathcal{A}}$ erhält die Challenge $(\mathsf{trans}, K_b, K_{1-b})$ anstelle von (trans, K_b), d.h. $\widetilde{\mathcal{A}}$ bekommt den korrekt erzeugten *und* den zufällig gewählten Schlüssel als Eingabe und muss entscheiden, in welcher Reihenfolge er diese erhalten hat. Wir betrachten also das modifizierte Spiel $\widetilde{\mathsf{KE}}_{\widetilde{\mathcal{A}},\Pi}(n)$:



Zeigen Sie, dass die beiden Definitionen äquivalent sind, d.h. konstruieren Sie aus einem Angreifer $\widetilde{\mathcal{A}}$ bzgl. $\widetilde{\mathsf{KE}}_{\widetilde{\mathcal{A}},\Pi}(n)$ einen Angreifer $\mathcal{A}$ für $\mathsf{KE}_{\mathcal{A},\Pi}(n)$ und umgekehrt. Analysieren sie den Vorteil.

AUFGABE 2. Konstruktives. (5 Punkte)
Zeigen Sie, dass jedes 2-Runden-Schlüsselaustauschprotokoll Π, welches sicher gegen passive Angreifer ist, in ein CPA-sicheres Public-Key Verfahren $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ transformiert werden kann, d.h. zeigen Sie sowohl die Korrektheit Ihres Verfahrens als auch die CPA-Sicherheit.

AUFGABE 3. Randomisierung. (5 Punkte)
Sei $N = pq$ ein fester Modul bestehend aus zwei Primzahlen p, q. Nehmen Sie an, dass es einen Angreifer $\mathcal{A}$ gibt, der zur Eingabe (N, e) und $x^e \bmod N$ in Laufzeit t die e-te Wurzel mit einer Erfolgswahrscheinlichkeit von 0.01 berechnet, d.h.

$$\mathbf{Pr}_{x \in_R \mathbb{Z}_N^*} [\mathcal{A}(N, e, x^e \bmod N) = x] = 0.01,$$

wobei die Wahrscheinlichkeit über die zufällige Wahl $x \leftarrow \mathbb{Z}_N^*$ geht.
Zeigen Sie, dass es möglich ist, daraus einen Angreifer $\mathcal{A}'$ zu konstruieren, der Laufzeit $t' = \mathsf{poly}(\log_2 N, t)$ hat und für den

$$\mathbf{Pr} [\mathcal{A}'(N, e, x^e \bmod N) = x] = 0.99$$

gilt.

AUFGABE 4. Padding. (5 Punkte)
Sei GenRSA ein Algorithmus zur RSA-Schlüsselerzeugung (siehe auch Folie 36). Betrachten Sie das folgende Experiment $\mathsf{PAD}_{\mathcal{A},\mathsf{GenRSA},\ell}$ für einen ppt-Algorithmus $\mathcal{A}$ und eine Funktion $\ell(n) \leq 2n - 2$ (für alle $n \in \mathbb{N}$):

i) $(N, e, d) \leftarrow \mathsf{GenRSA}(1^n)$

ii) $m \leftarrow \mathcal{A}(N, e)$ wobei $m \in \{0,1\}^{\ell(n)}$

iii) Wähle $y_0 \in_R \mathbb{Z}_N^*$ und $r \in_R \{0,1\}^{\log_2 N - \ell(n) - 1}$ und setze $y_1 := (r||m)^e \mod N$

iv) Wähle $b \in_R \{0,1\}$ und sende y_b an $\mathcal{A}$. Sei $b' \leftarrow \mathcal{A}(N, e, y_b)$

v) Gib 1 aus genau dann, wenn $b = b'$

Wir sagen, dass das ℓ-padded-RSA Problem hart ist bezüglich GenRSA, wenn für jeden ppt-Angreifer $\mathcal{A}$ gilt

$$\mathbf{Pr} [\mathsf{PAD}_{\mathcal{A},\mathsf{GenRSA},\ell}(n) = 1] \leq \frac{1}{2} + \mathsf{negl}(n)$$

Zeigen Sie: Wenn das ℓ-padded RSA Problem hart ist bzgl. GenRSA, so ist auch das padded RSA-Verschlüsselungsverfahren (siehe Folie 39) CPA-sicher (wobei obiges ℓ verwendet wird).